KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Otto Dufva

VERKKOLAITTEIDEN ETÄHALLINNAN TODENTAMINEN

Opinnäytetyö 2014

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

DUFVA, OTTO	Verkkolaitteiden etähallinnan todentaminen
Opinnäytetyö	32 sivua + 2 liitesivua
Työn ohjaaja	Lehtori Jouko Pahlama
Toimeksiantaja	Kymenlaakson ammattikorkeakoulu Oy
Huhtikuu 2014	
Avainsanat	RADIUS, AAA, todentaminen, Active Directory

Tämän opinnäytetyön tavoitteena oli luoda Kyamkin ICT-LABin tietoverkkoon aktiivilaitteiden hallintayhteyksiä valvova keskitetty käyttäjien todentamisratkaisu. Sillä oli tarkoitus parantaa verkkolaitteiden tietoturvaa merkittävästi.

Tietoverkkoihin kohdistuvien uhkien lisääntyminen on tehnyt verkkojen ja tietojen turvaamisesta entistä haastavampaa. Verkkoturvallisuuden ylläpitämien vaatii verkon ylläpitäjiltä yhä enemmän huomiota kaikilla verkon osa-alueilla. Kymenlaakson ammattikorkeakouluun tuleva kyberturvallisuuslaboratorio asettaa uusia vaatimuksia myös koko muun verkon tietoturvalle.

Kyamkin Tietotekniikan tuotantoverkossa verkkolaitteiden hallintayhteyksiin liittyvä käyttäjien kirjautumisen valvonta toteutettiin ottamalla käyttöön RADIUS-todentaminen. Palvelimena toimii Microsoftin Network Policy Server, joka on Windows Server 2008 R2 -palvelinkoneessa. Käyttäjätietokantana toimii samassa koneessa pyörivä Active Directory -tietokanta, johon luotiin uusi käyttäjäryhmä. Vain siihen kuuluvien henkilöiden on sallittua muodostaa hallintayhteys verkon laitteisiin. Tähän ryhmään voidaan helposti tarpeen tullen lisätä tai poistaa käyttäjiä.

Opinnäytetyön tuloksena tuotantoverkon tietoturva parani huomattavasti, koska aktiivilaitteiden hallintayhteyksien muodostamista voidaan nyt rajata ja tapahtuneet kirjautumiset tallentuvat tietokantaan. IPv4-osoitteilla todennus saatiin toimimaan luotettavasti, mutta IPv6-verkon osalta toteutus jäi tekemättä.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information Technology

DUFVA, OTTO	Authentication of Network Devices' Remote Access
Bachelor's thesis	32 pages + 2 pages of appendices
Supervisor	Jouko Pahlama, Senior Lecturer
Commissioned by	Kymenlaakso University of Applied Sciences
April 2014	
Keywords	RADIUS, AAA, authentication, Active Directory

The goal of this study was to create a centralized user authentication for the management access of the network devices in KyUAS ICT-LAB's network devices. This was to increase the security of network devices significantly.

The growth of threats against networks has made securing of networks and information more demanding. Maintaining network security requires more attention from the network administrator in all sections of the network. The upcoming cyber security laboratory in Kymenlaakso UAS sets new security requirements for the rest of the network.

RADIUS-authentication was implemented into the network devices of Kymenlaakso UAS Information Technology department's production network to control management access. The server is Microsoft Network Policy Server that runs on a Windows Server 2008 R2 server. The user database is the Active Directory database that runs on the same machine. A new user group was created into the existing database. Only members of this group are granted management access to the network devices. User can be easily added and removed to this group if needed.

As a result, the production network's security was improved greatly by limiting management access to the devices and logins are recorded in the database. The authentication was implemented reliably by using IPv4-addresses, but implementation to the IPv6 section of the network was not made.

SISÄLLYS

LYHENNELUETTELO

AAA	Authentication, Authorization and Accounting: malli tietoverkkojen todennukseen, valtuutukseen sekä tilastointiin
AD	Microsoft Active Directory
CHAP	Challenge Handshake Authentication Protocol
IETF	Internet Engineering Task Force
IOS	Internetwork Operating System: Cisco Systemsin laitteiden käyttämä käyttöjärjestelmä
MD5	Message-Digest: yleisesti käytössä oleva salauksissa käytetty tiivistealgoritmi
MS-CHAP	Microsoft CHAP Extensions: Microsoftin ominaisuuksiin mukautettu CHAP
NAS	Network Access Server: verkkoon kirjautumista valvova laite, joka voi olla esimerkiksi Kytkin tai Langaton tukiasema
OSI	Open Systems Interconnection: seitsenkerroksinen avoin järjestelmämalli
PAP	Password Authentication Protocol
PIN	Personal Identification Number
RADIUS	Remote Authentication Dial In User Service: RFC-dokumentin määrittämä standardi, joka tarjoaa todennusta, valtuutusta sekä kirjanpitoa
RFC	Request for Comments: IETF:n julkaisu

RSA	Julkisen avaimen salausalgoritmi
SSH	Secure Shell: salattuun tietoliikenteeseen tarkoitettu protokolla
UDP	User Datagram Protocol: TCP/IP-protokollaperheen varmistamaton kuljetusprotokolla
VLAN	Virtual Local Area Network: virtuaalilähiverkko, jolla voidaan jakaa yksi fyysinen tietoliikenneverkko useampaan loogiseen osaan
VPN	Virtual Private Network: virtuaalinen erillisverkko, jolla voidaan yhdistää kaksi erillistä lähiverkkoa julkisen verkon yli toisiinsa

1 JOHDANTO

Tietoverkkojen tietoturvauhkien määrä lisääntyy jatkuvasti. Näihin uhkiin täytyy varautua parantamalla tietoverkkojen tietoturvan tasoa. Tietoturvan täytyy ylettyä verkon jokaiseen osaan. Verkkoliikennettä välittävät laitteet saattavat helposti jäädä tietoturvamielessä liian vähäiselle huomiolle ajatellen vaikkapa etähallintayhteyden kautta laitteisiin kirjautumassa olevan henkilön käyttöoikeuden varmistamista. Kuitenkin verkon aktiivilaitteet ovat eräs verkon kriittisimmistä osista tietoturvan suhteen. Mikäli luvaton käyttäjä pääsee verkkolaitteisiin käsiksi, näkyy kaikki verkon liikenne hänelle. Tunkeutuja voi myös tehdä omia määrityksiään laitteisiin.

Mahdollisten luvattomien kirjautumisten estämiseksi on laitteiden hallintayhteyksien muodostamisen valvonta hyvä suorittaa keskitetysti ilman tunnettuja salasanoja. Tällöin verkon aktiivilaitteet määritellään käyttämään ulkopuolista todennuspalvelinta käyttäjien kirjautumisoikeuksien hallintaan. Kun aktiivilaitteisiin kirjautuminen yhdistetään samaan tietokantaan kaiken muun verkkokirjautumisen kanssa, voidaan samoilla, usein olemassa olevilla Active Directory -tunnuksilla kirjautua myös verkkolaitteisiin. Samalla saadaan myös talletettua tietoa laitteisiin kirjautuneista käyttäjistä.

Opinnäytetyön tarkoituksena on huolellisesti tutustua RADIUS-protokollan toimintaan, AAA-malliin yleisesti sekä dokumentoida se, miten todennus tehdään käyttäen hyväksi Active Directoryn -tietokantaa. Dokumentin alussa käsitellään RADIUS-protokollaa ja AAA-mallia. Tekninen toteutus tehdään Kymenlaakson ammattikorkeakoulun Tietotekniikan siiven verkkoon, jossa käytetään Cisco Systemsin valmistamia verkon aktiivilaitteita.

2 AAA-MALLI

Tietoverkkojen autentikointiin tarkoitettu AAA-prosessi (Authentication, Authorization and Accounting) on kehitetty jo ennen nykyistä Internetiä. Todentaminen (Authentication) varmistaa asiakkaan henkilöllisyyden. Valtuuttaminen (Authorization) määrittelee, mitä asiakas saa tehdä. Tilastointi (Accounting) tekee kirjanpitoa toimenpiteistä kirjautumisen kuluessa. (1.)

2.1 Authentication

Todennusta tehtäessä useita eri tekijöitä voidaan tarkastella, ennen kuin todennuspalvelin päättää pääsyn verkkoon. Korkealla tasolla nämä voidaan jakaa kolmeen ryhmään: asiakas, asiakkaan valtakirja sekä asiayhteydessä ilmenevät tiedot. (1.)

2.1.1 Asiakas

Asiakas on kokonaisuus, joka pyytää valtuutuksia. Yleisesti asiakas on yhdistelmä käyttäjästä, laitteesta tai palvelusta. Käyttäjän ja laitteen todennus voidaan tarjota peräkkäin samaan todennustapahtumaan, sisältäen usein ensin laitteen tunnistuksen ja käyttäjän tunnistuksen tämän jälkeen. (1.)

2.1.2 Valtakirja

Asiakkaan valtakirjat voidaan jakaa neljään ryhmään: salasana, kertakäyttöinen salasana, digitaalinen sertifikaatti sekä biometrinen tunnistautuminen. (1.)

Salasana on yleisimmin käytetty valtakirja. Salasanan varmistamiseen voidaan käyttää eri protokollia. PAP on selkokielistä todennusta, jonka käyttö ei ole suositeltavaa. Uudet protokollat tosin tarjoavat suojatun kuljetuksen PAP-protokollalle, tehden siitä edelleen käytetyn AAA-prosessissa. CHAP lisää turvallisuutta PAP-protokollaan verrattuna lähettämällä salasanan sijaan haasteen, joka perustuu salasanasta laskettuun tiivisteeseen. MS-CHAP on Microsoftin laajennus CHAP-protokollaan, joka muokkaa siitä sopivamman Microsoft-ympäristöihin. Salasanat ovat kaikissa muodoissaan alttiita sanakirjahyökkäyksille, koska varsinkin heikot salasanat voidaan hyökkäyksillä selvittää ja niiden tiiviste laskea. (1.)

Tietoturva paranee, jos käytössä on kertakäyttöinen salasana, jonka käyttäjä kirjautuessaan syöttää. Verkkoon kirjautujalla on hallussaan henkilökohtainen turvamoduuli, joka generoi sattumanvaraisen salasanan. Se on synkronoitu tietoturvapalvelimen kanssa. Tällainen salasana voidaan lähettää selkokielisenä, koska sitä käytetään vain kerran. Määritellyn ajan jälkeen generoidaan uusi salasana. Kun kertakäyttöiseen salasanaan yhdistetään PIN-koodin (Personal Identification Number) käyttö, saavutetaan kahden tekijän todennus. Tällöin käyttäjällä täytyy olla jotain (turvamoduuli) ja hänen pitää tietää jotain (PIN-koodi). (1.)

Digitaalinen sertifikaatti voi olla paikallisesti laitteessa tai jokin irrotettava laite kuten älykortti. Käyttäjän identiteetti varmistetaan vaatimalla sertifikaatille allekirjoitus tunnetulta sertifikaatti auktoriteetilta. Sertifikaatti itsessään voidaan jakaa vapaasti, koska se vaatii aina henkilökohtaisen avaimen. Koska henkilökohtainen avain sijaitsee asiakkaassa, sertifikaatteja käytetään yleisimmin todentamaan laitetta ihmisen sijaan. Älykortit tosin muuttavat asiaa mahdollistamalla käyttäjän ottaa sertifikaatti sekä henkilökohtainen avain mukaansa. Kertakäyttöisen salasanan tapaan sertifikaatti ei yksin tarjoa kahden tekijän todennusta. Tämä ratkaistaan vaatimalla PIN-koodi älykorttiin käsiksi pääsemiseen. (1.)

Biometrinen tunnistautuminen on vähiten käytetty tunnistusmenetelmä. Biometriikka ei välitä siitä, mitä asiakas omaa tai tietää, vaan keskittyy siihen mitä asiakas on. Sormenjälkitunnistimet, iirisskannerit sekä kasvojentunnistus ovat kaikki biometrisen todentamisen muotoja. (1.)

2.1.3 Asiayhteys

Tunnistustietoja lähetettäessä voidaan myös lähettää tietoja siitä, missä asiakas on ja millaisella laitteella verkkoon kirjaudutaan. Tällaisia tietoja ovat fyysinen sijainti, verkkosijainti ja kellonaika. Melko uutena tekijänä voidaan myös tarkastaa asiakaskoneen sovellusten tila ennen yhdistämistä (Network Access Protection). Asiakaskoneen riskiuhka voidaan määrittää ennen yhteyden sallimista asiakkaalle. (1.)

2.2 Authorization

Valtuuttamisella (Authorization) määritellään, mitä asiakas saa tehdä verkossa. Tätä määrittelyä voidaan tehdä monella eri tasolla lähtien siirtokerroksen (Layer 2) VLAN-pohjaisista rajoituksista aina sovelluskerroksen (Layer 7) oikeutuksiin. (1.)

2.2.1 Ei valtuutusta

Yleinen tapa on tehdä todennusta ilman mitään valtuutusta. Kun todentaminen on suoritettu, saa käyttäjä täydet oikeudet verkkoon. Tämä on jäänne vanhasta etäyhteyden muodostamiseen liittyneen valvonnan tavoitteesta, missä vain määriteltiin oliko asiakas luotettava vai ei. (1.)

2.2.2 Siirtokerroksen osiointi

Langattoman verkon tukiasemille ja lähiverkon kytkimille tyypillisin tapa on suorittaa verkossa kulkevan liikenteen jakamista eri käyttäjäryhmien kesken siirtokerroksella. Silloin verkko jaetaan useaan loogiseen osaan, jotta eri osien liikenne voidaan erottaa toisistaan. Tämä toteutetaan yleisesti ottamalla käyttöön virtuaalisia lähiverkkoja (VLAN), jotka jakavat samassa fyysisessä verkossa olevat käyttäjät erillisiin kuvitteellisiin lähiverkkoihin. Virtuaalilähiverkkoja taas pystytään käyttämään liikenteen suodatukseen ja määrittelemään mitä oikeuksia tietyn virtuaaliverkon käyttäjille annetaan. (1.)

2.2.3 Verkkokerroksen suodattaminen

Verkkokerroksella liikennettä voidaan suodattaa käyttämällä pääsylistoja (Access Control Lists). Niiden avulla voidaan liikennettä suodattaa verkko-osoitteen ja sovelluksen käyttämän porttinumeron perusteella erikseen sekä tulo- että lähtösuuntaan. Pääsylistoja voidaan yhdistää siirtokerroksen osiointiin tarjoamaan yhdistettyjä valtuutuksia koko virtuaalilähiverkolle. (1.)

2.2.4 Sovelluskerroksen oikeutukset

Kun tietoturvalaitteet ovat kehittyneet, ne pystyvät tarkastelemaan liikennettä myös OSI-mallin ylempien kerrosten osalta. Tarkkailemalla OSI-mallin ylimmän kerroksen tietoja, voidaan sallia pääsy vain tiettyihin sovelluksiin. (1.)

2.3 Accounting

Tilastoinnin tärkeys kasvaa tietoverkoissa. Yhdistettynä verkon muiden laitteiden dataan, voidaan pitää tarkkaa kirjaa milloin asiakas on yhdistänyt verkkoon, mitä tämä tekee verkossa sekä milloin tämä on poistunut verkossa. Saavutettua tietoa voidaan käyttää tutkittaessa, mitä asiakas on tehnyt verkossa ja vertailtaessa, mitä tämä saisi tehdä. (1.)

Tilastointi on laajalti palveluntarjoajien käytössä. Sen avulla voidaan laskuttaa asiakasta ja tarkastella asiakkaan toimintaa. (1.)

3 RADIUS

Remote Authentication Dial-In User Service (RADIUS) on yleisesti käytössä oleva protokolla, joka tarjoaa tietoverkon käyttäjiin liittyvää todennusta, valtuutusta ja kirjanpitoa. RADIUS-protokollaan perustuva verkon aktiivilaitteiden etähallintayhteyksien valvonta sisältää yleensä neljä komponenttia: käyttäjän, asiakkaan eli autentikointilaitteen (RADIUS Client), todennuspalvelimen (RADIUS Server) sekä mahdollisesti erillisen tietokantapalvelimen. (2.)

RADIUS-protokollan on kehittänyt Livingston Enterprises, Inc alun perin sisäänsoittopalveluiden todentamiseen ja valtuuttamiseen. Nykyinen RADIUS-protokolla on määritelty IETF:n (Internet Engineering Task Force) julkaisemissa RFC-dokumenteissa RFC2865 ja RFC2866. (3.)(4.)

3.1 Yleistä

RADIUS toimii asiakas-palvelin-mallilla. NAS (Network Access Server) toimii asiakkaana RADIUS-palvelimelle. NAS välittää kirjautujaa koskevat tiedot RADIUS-palvelimelle sekä toimii saamansa vastauksen mukaisesti. RADIUS-palvelin on valmiina vastaanottamaan käyttäjän yhteydenmuodostuspyyntöjä, todentamaan käyttäjän sekä lähettämään kaiken tarvittavan konfigurointitiedon asiakkaalle, jotta tämä voi tarjota palvelua käyttäjälle. RADIUS-palvelin voi toimia välityspalvelimena toisille RADIUS-palvelimille tai muille todennuspalvelimille. (4.)

NAS-laitteen ja RADIUS-palvelimen väliset yhteydet suojataan käyttäen jaettua avainta, jota ei koskaan lähetetä verkon yli. Lisäksi kaikki käyttäjien salasanat lähetetään salattuna. (4.)

3.2 Rajoitteet

RADIUS sisältää myös rajoitteita. Yksi niistä on se, että käytettäessä RADIUS-välityspalvelimia, näkyy kaikki tieto jokaisessa välissä olevassa palvelimessa riippumatta salauksesta. Salasanojen ja sertifikaattien siirtämiselle tämä ei ole riittävän turvallista. (5.)

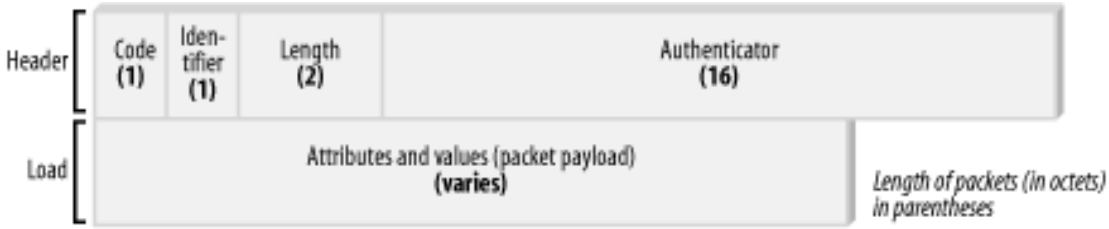
Toinen rajoite on se, että RADIUS on tilaton, eikä täten seuraa kokoonpanoasetuksia tai tapahtumatietoja seuraavaa yhteyttä varten. (5.)

Kokemukset ovat osoittaneet, että RADIUS skaalautuu huonosti suurempiin järjestelmiin. Tämä johtuu osin ruuhkautumista estävien säännöstöjen puutteesta. (4.)

3.3 Paketit

3.3.1 Pakettien muodot

RADIUS-protokolla käyttää UDP-paketteja asiakkaan ja palvelimen väliseen liikenteeseen. RADIUS käyttää todennukseen porttia numero 1812. Aluksi käytettiin porttia numero 1645, mutta se muutettiin ristiriidan vuoksi. RADIUS-pakettien rakenne on jaettu kuvan 1 mukaisesti viiteen osaan. (5.)



Kuva 1. RADIUS-pakettien rakenne. Suluissa on kentän pituus tavuina. (1.)

Koodiosa (Code) on yhden tavun mittainen ja erottaa minkä tyyppisestä RADIUS-viestistä on kyse. Väärällä koodilla varustetut paketit hylätään ilman mitään ilmoitusta. Sallitut koodit ovat:

1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (under continued development)
13	Status-Client (under continued development)
255	Reserved (1.)

Tunnisteosa (Identifier) on yhden tavun mittainen. Se auttaa yhdistämään keskenään pyynnöt ja niihin liittyvät vastaukset. RADIUS-palvelin voi tunnistaa lyhyen ajan sisällä toisen samanlaisen pyynnön, jos sillä on sama asiakkaan IP-osoite, lähde UDP-portti sekä tunniste. (4.)

Pituusosa (Length) on pituudeltaan kaksi tavua. Se ilmaisee koko paketin pituuden sisältäen kaikki paketin osat. Tavut, jotka ovat pituusosan ilmoittaman alueen ulkopuolella, täytyy tulkita täytteeksi ja jättää huomioimatta vastaanotettaessa. Jos paketti on pituusosan ilmoittamaa mittaa lyhyempi, se täytyy hylätä ilmoituksetta. Paketin pienin pituus on 20 tavua ja suurin pituus 4096 tavua. (4.)

Todennusosa (Authenticator) on 16 tavun pituinen. Eniten merkitsevä tavu lähetetään ensimmäisenä. Tätä arvoa käytetään sekä todentamaan RADIUS-palvelimen lähettämä vastaus että piilottamaan salasana käyttäen tarvittavaa algoritmia. (4.)

Yhteyspyyntöön käytetty todennusosa on 16 tavun pituinen satunnaisluku, jonka arvon tulisi olla ennalta arvaamaton sekä uniikki jaetun avaimen elinajan. Koska on odotettavissa, että samaa avainta saatetaan käyttää todentamiseen eri maantieteellisen sijainnin omaavien palvelinten kanssa, tulisi arvon omata globaalia ja ajallista ainutlaatuisuutta. (4.)

Edellä mainittu vaatimus huomioiden vastaukseen käytetty todennusosa on MD5-algoritmilla laskettu tiiviste koodiosasta, tunnisteosasta, pituusosasta, yhteyspyynnön todennusosasta, vastauksen attribuuteista sekä jaetusta avaimesta. (4.)

3.3.2 Pakettien tyypit

RADIUS-paketin tyyppi määritellään paketin koodiosassa. Neljä pakettityyppiä on merkityksellisiä todennus- ja valtuutusvaiheissa. (4.)(5.)

3.3.2.1 Access-Request

Yhteyspyyntöä (Access-Request) käytetään, kun käyttäjä pyytää tiettyä palvelua verkosta. Asiakas lähettää yhteyspyynnön RADIUS-palvelimelle pyydettyjen palveluiden listan kanssa. RFC-dokumenttien mukaan vastaus täytyy lähettää jokaiseen oikeutettuun yhteyspyyntöön, riippumatta onko vastauksena hylkäys tai valtuutus. (5.)

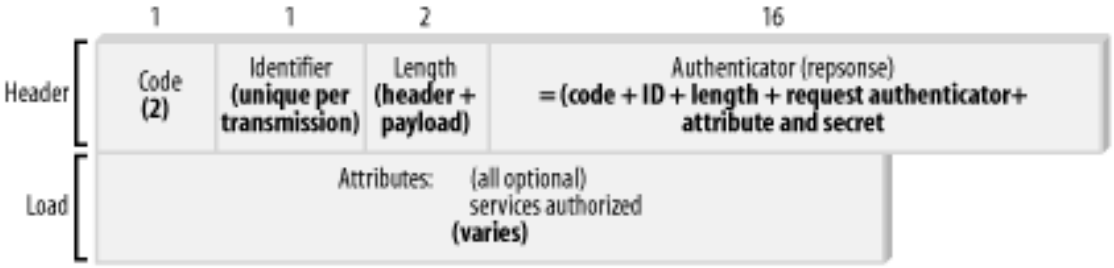
Yhteyspyynnön tietosisällön tulisi sisältää käyttäjänimi-attribuutti pääsyä hakevan henkilön tunnistamiseksi, sekä pääsyä hakevan verkkolaitteen IP-osoite tai ensisijainen verkkonimi. Lisäksi sisällön mukana on oltava salasana, joka on kryptattu MD5-algoritmilla. Kuva 2 esittää yhteyspyyntöpaketin rakenteen. (5.)

Kuva 2. Access-Request-paketin rakenne (5.)

3.3.2.2 Access-Accept

Hyväksymisviesti (Access-Accept), joita RADIUS-palvelin lähettää asiakkaalle, tunnustaa käyttäjän pääsyn sallimisen. Jotta pyyntö- ja vastauspaketit voidaan yhdistää oikein, täytyy tunnisteosien olla identtiset molemmissa paketeissa. (5.)

Paketin tietosisältö on niin suuri tai pieni, kuin on tarvetta. Todennäköisesti attribuutit kertovat, mihin palveluihin käyttäjällä on oikeus. Jos kuitenkaan ei lähetetä mitään attribuutteja, asiakas olettaa kaikkien pyydettyjen palveluiden olevan sallittuja. Kuva 3 esittää hyväksymisviestin rakenteen. (5.)



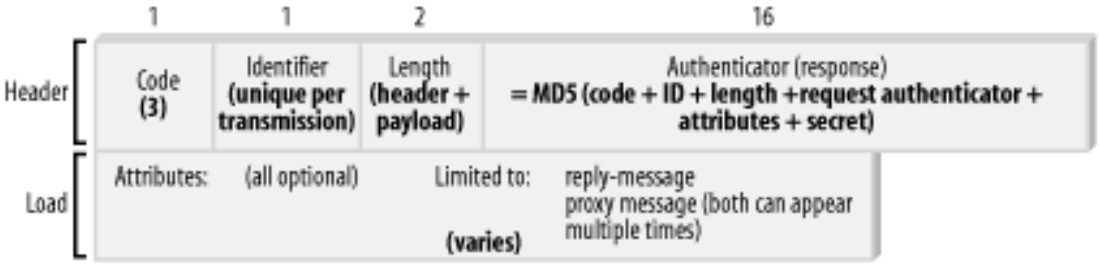
Kuva 3. Access-Accept-paketin rakenne (5.)

3.3.2.3 Access-Reject

RADIUS-palvelimen täytyy lähettää asiakkaalle hylkäysviesti (Access-Reject), mikäli jokin yhteyspyynnön palveluista hylätään. Hylkäys voi perustua järjestelmän politiikkoihin, vaillinaisiin valtuutuksiin tai mihin tahansa muihin vaatimuksiin. Hylkäysvies-

ti voidaan lähettää millä tahansa hetkellä yhteysjakson aikana, mikä tekee siitä ihanteellisen yhteyden aikarajoitteiden määrittämiseen. (5.)

Hylkäysviestin tietosisältö on rajoitettu kahteen attribuuttiin, jotka voivat tosin esiintyä useamman kerran. Sallitut attribuutit ovat vastausviesti, joka voidaan näyttää käyttäjälle, sekä Proxy-State-attribuutit. Näiden attribuuttien lisäksi hylkäysviestissä ei voi esiintyä mitään muita attribuutteja. Kuva 4 esittää hylkäysviestin rakenteen. (5.)

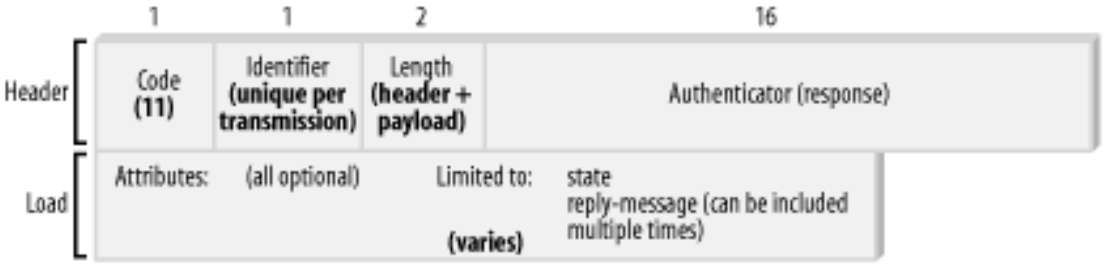


Kuva 4. Access-Reject-paketin rakenne. (5.)

3.3.2.4 Access-Challenge

Haasteviesti voidaan lähettää, jos palvelin saa ristiriitaista tietoa tai haluaa vain vähentää virheellisen todennuksen riskiä. Saadessaan haasteviestin asiakas joutuu lähettämään uuden yhteyspyynnön, joka sisältää tarkoituksen mukaisen tiedon. Jotkin asiakaslaitteet eivät tue haasteviestiä, jolloin se käsitellään hylkäysviestinä. (5.)

Haasteviestin tietosisältö on myös rajoitettu kahteen attribuuttiin. Vastausviesti, joka voidaan näyttää käyttäjälle, voi esiintyä paketissa useamman kerran. Tila-attribuutti (State) voi esiintyä vain kerran. Se kopioidaan muuttamattomana uuteen yhteyspyyntöön, joka lähetetään haasteen lähettäneelle palvelimelle. Kuva 5 esittää haasteviestin rakenteen. (5.)



Kuva 5. Access-Challenge-paketin rakenne (5.)

3.4 RADIUS toiminta

Kun asiakas (NAS-laite) on määritelty käyttämään RADIUSta, kaikki sen käyttäjät lähettävät todennustiedot asiakkaalle. (4.)

Kun asiakas on saanut todennustiedot, se voi valita todennuksen RADIUS-toiminnan avulla. Tätä varten asiakas luo yhteyspyynnön, joka sisältää käyttäjänimen, salasanan, käyttäjän koneen tunnisteen sekä porttitunnisteen sille portille, jonka kautta käyttäjä on kirjautumassa verkkoon. Salasanat suojataan käyttäen MD5-algoritmia. (4.)

Yhteyspyyntö (Access-Request) lähetetään RADIUS-palvelimelle. Mikäli vastausta ei saada tietyn ajan kuluessa, pyyntö lähetetään uudelleen. Asiakas voi myös lähettää pyynnön varapalvelimelle tai varapalvelimille, mikäli ensisijaiseen palvelimeen ei saada yhteyttä. Varapalvelinta voidaan käyttää, kun tarpeeksi monta pyyntöä ensisijaiselle palvelimelle epäonnistuu tai käyttäen kiertoperiaatetta. (4.)

Kun RADIUS-palvelin vastaanottaa pyynnön, se vahvistaa lähettävän asiakkaan. Pyynnöt asiakkailta, joille palvelimella ei ole jaettua avainta, täytyy hylätä ilman ilmoitusta. Mikäli asiakas vahvistetaan, RADIUS-palvelin vertaa tietokantaan löytääkseen pyyntöä vastaavan käyttäjän. Käyttäjän tietomerkintä sisältää vaatimukset, joiden tulee täyttyä yhteyden sallimiseen. (4.)

Mikäli jokin ehto ei toteudu, RADIUS-palvelin lähettää hylkäysviestin (Access-Reject) kertoen käyttäjän pyynnön olevan mitätön. Haluttuaan palvelin voi lähettää tekstiä viestissä, jonka asiakas voi näyttää käyttäjälle. Mitään muita attribuutteja (paitsi Proxy-State) ei sallita Access-Reject-pakettiin. (4.)

Jos kaikki ehdot täyttyvät, voi RADIUS-palvelin halutessaan lähettää käyttäjälle haasteen. Haaste (Access-Challenge) voi sisältää tekstiä, johon käyttäjän tulee vastata. Tämä viesti lähetetään asiakkaalle, joka voi näyttää sen käyttäjälle. Käyttäjän vastauksen jälkeen palvelin voi lähettää sen perusteella uuden haasteen, hylkäysviestin (Access-Reject) tai hyväksymisviestin (Access-Accept). (4.)

Kun kaikki ehdot toteutuvat, käyttäjälle lähetetään hyväksymisviestissä lista määrittelytiedoista. Nämä tiedot sisältävät palvelun tyypin sekä kaikki tarvittavat tiedot halutun palvelun tarjoamiseksi. (4.)

3.4.1 Haaste-vastaus

Haaste-vastaus -todennuksessa käyttäjälle annetaan ennalta arvaamaton numero ja haaste salata se, sekä lähettää vastaus takaisin. Todennetut käyttäjät ovat varustettu erikoislaitteilla kuten älykorteilla tai ohjelmalla, joka toteuttaa oikean vastauksen laskemisen helposti. Todentamattomat asiakkaat, ilman oikeanlaista laitetta tai ohjelmaa sekä tietoa jaetusta avaimesta muodostaakseen itse tällaisen ohjelman, voivat vain arvata vastaukseen. (4.)

Haasteviesti sisältää tyypillisesti haasteen sisältävän vastausviestin, joka näytetään käyttäjälle. Tällainen haaste on esimerkiksi numeerinen arvo, jota ei todennäköisesti koskaan toisteta. Tyypillisesti tällainen saadaan ulkoiselta palvelimelta, joka tietää, millainen todennuslaite todennetulla käyttäjällä on, ja valitsee sopivan pituisen satunnaisluvun. (4.)

Käyttäjä syöttää saadun luvun laitteeseensa tai ohjelmaansa, joka laskee vastauksen. Tämän vastauksen käyttäjä lähettää takaisin asiakkaalle, joka lähettää sen edelleen RADIUS-palvelimelle toisessa yhteyspyynnössä. Mikäli tämä vastaus täsmää odotetun vastauksen kanssa, lähetetään hyväksymisviesti, muissa tapauksissa hylkäysviesti. (4.)

3.5 Proxy RADIUS

RADIUS-välityspalvelimen toiminnassa yksi RADIUS-palvelin vastaanottaa todennus- tai tilastointipyynnön asiakkaalta. Tämä palvelin edelleen lähettää pyynnön etäiselle RADIUS-palvelimelle, vastaanottaa viestin etäpalvelimelta sekä lähettää vastauksen asiakkaalle. Vastauksessa on mahdollista olla muutoksia vastaamaan paikallista hallintopolitiikkaa. Yleinen käyttö tällaiselle toiminnalle on verkkovierailu. Verkkovierailu mahdollistaa kahden tai useamman hallintoyksikön päästää toistensa käyttäjiä toisen yksikön verkkoon. (4.)

RADIUS-palvelin voi toimia sekä välittävänä palvelimena että etäpalvelimena. Palvelin voi toimia välittävänä palvelimena yhdelle alueelle ja etäpalvelimena toiselle alueelle. Yksi välittävä palvelin voi toimia välittäjänä usealle etäpalvelimelle. Useat välittävät palvelimet voivat käyttää samaa etäpalvelinta, joka voi tarjota todennusta useille eri alueille. Yksi välittävä palvelin voi välittää viestin edelleen seuraavalle välittävälle

palvelimelle. Näin muodostuu välittäjien ketju, jolloin täytyy varoa muodostamasta silmukoita. (4.)

Välittävän palvelimen täytyy lähettää kaikki paketin sisältämät Proxy-State -attribuutit läpi sellaisenaan koskematta niihin. Välittävän palvelimen toiminta ei saa riippua muiden välittävien palvelimien lisäämien Proxy-State -attribuuttien sisällöstä. Jos asiakkaan lähettämässä pyynnössä on yhtään Proxy-State -attribuutteja, välittävän palvelimen tulee sisällyttää samat attribuutit vastaukseensa asiakkaalle. Välittävä palvelin voi sisällyttää Proxy-State -attribuutit välittämäänsä yhteyspyyntöön tai jättää ne pois välittämässään pyynnössä. Jos välittävä palvelin jättää attribuutit pois välittämässään yhteyspyynnössä, ne on palautettava takaisin paikoilleen ennen vastauksen lähettämistä asiakkaalle. Välittävä palvelin voi joutua muokkaamaan attribuutteja noudattaakseen paikallista politiikkaa. Välittäjä ei kuitenkaan saa muuttaa Proxy-State-, State- tai Class-attribuutteja, joita paketti sisältää. (4.)

3.6 UDP-protokollan käyttö

RADIUS käyttää UDP-protokollaa TCP-protokollan sijaan. Tämä valinta on tehty ainoastaan teknisistä syistä. UDP:n käyttäminen kuitenkin edellyttää erillisenä määrittelynä yhden sellaisen toiminnon hoitamista, joka on sisäänrakennettuna TCP:hen. UDP:n kanssa täytyy keinotekoisesti hallita uudelleenlähetysajoituksia samalle palvelimelle. Tämä on pieni hinta saavutetuista hyödyistä, joita UDP tarjoaa. (4.)

3.6.1 Ajoitukset

Jos pyyntö ensisijaiselle palvelimelle epäonnistuu, pyyntö lähetetään toissijaiselle palvelimelle. Tämän vaatimuksen täyttymiseksi kopio pyynnöstä on säilytettävä kuljetuskerroksen yläpuolella, jotta lähetys toissijaiselle palvelimelle pystytään tarvittaessa toteuttamaan. Tämän vuoksi tarvitaan edelleen uudelleenlähetyksen ajastimia. (4.)

RADIUS-protokollan ajoitusvaatimukset ovat merkittävästi erilaisia kuin mitä TCP-protokolla tarjoaa, sillä RADIUS ei vaadi reagoivaa tunnistamista menetetylle tiedolle. Käyttäjä voi odottaa muutaman sekunnin, jotta todennus onnistuu, mutta käyttäjä ei ole halukas odottamaan useita minuutteja todennuksen onnistumista. Tästä syystä TCP:n tarjoama luotettava kuljetus parin minuutin kuluttua ei ole käytännöllistä. No-

peampi toissijaisen palvelimen käyttö mahdollistaa käyttäjän todennuksen, ennen kuin käyttäjä luopuu yhteysyrityksestä. (4.)

3.6.2 Tilattomuus

Asiakkaita ja palvelimia lisätään ja poistetaan. Järjestelmiä käynnistetään ja sammutetaan itsenäisesti. Yleisesti tämä ei aiheuta ongelmia. Luovien ajoitusten ja kadonneiden TCP-yhteyksien tunnistaminen voidaan kirjoittaa koodiin, jotta voidaan käsitellä luonnottomia tapahtumia. UDP poistaa kokonaan tarvittavan erikoiskäsittelyn. Jokainen asiakas ja palvelin voivat avata UDP-yhteyden vain kerran ja jättää sen auki kaikkien järjestelmän vikatilanteiden ajaksi. (4.)

3.6.3 Yksinkertaisempi palvelinten käyttöönotto

Ensimmäisissä RADIUS-toteutuksissa palvelin oli yksisäikeinen. Tämä tarkoittaa että yksi pyyntö vastaanotettiin, käsiteltiin ja palautettiin. Tämä todettiin vaikeaksi hallita ympäristöissä, joissa tietoturvaratkaisut veivät aikaa. Palvelimen yhteyspyyntöjono täyttyi ja korkean käyttöasteen järjestelmissä pyyntöjen käsittelyaika kasvoi pidemmiksi kuin käyttäjät suostuivat odottamaan. Ilmeisen selvä ratkaisu oli tehdä palvelimista monisäikeisiä. Tämän saavuttaminen oli helppoa UDP:tä käyttäen. Eri prosesseja käynnistettiin palvelemaan jokaista pyyntöä, ja nämä prosessit pystyivät vastaamaan suoraan asiakkaalle yksinkertaisella UDP-paketilla alkuperäiseen viestiin. (4.)

3.7 Jaetut avaimet

Vahvistaakseen yhteyksien rikkomattomuutta, RADIUS-protokolla käyttää jaettujen avaimien (Shared Secret) käsitettä. Nämä ovat satunnaisesti generoituja arvoja, jotka ovat tunnettuja sekä asiakkaalla että palvelimella. Jaettuja avaimia käytetään kaikissa operaatioissa, jotka vaativat tiedon piilottamista ja arvojen salaamista. Ainoa tekninen rajoite on, että jaetun avaimen täytyy olla pituudeltaan yli nolla. Suosituksena on vähintään kuudentoista tavun mittaisten jaettujen avaimien käyttäminen. Niin pitkä avain on käytännössä mahdoton murtaa raa'alla voimalla (Brute Force). Samat säännöt, jotka koskevat salasanojen käyttöä, koskevat myös RADIUS jaettujen avainten käyttöä. Jaettujen avaimien tulisi olla uniikkeja tiettyyn RADIUS asiakas ja palvelin pariin. (5.)

Suuremman mittakaavan RADIUS-ratkaisuihin automaattinen jaettujen avaimien vaihtaminen vaikuttaisi järkevältä ratkaisulta. Tässä on kuitenkin suuri ansa, sillä ei ole takuuta asiakkaiden ja palvelinten pystyvän synkronoimaan uuden jaetun avaimen mahdollisimman hyvään aikaan. Vaikka samanaikainen synkronointi toteutuisi, olemassa olevia pyyntöjä saatettaisiin hylätä. Näin voisi tapahtua, mikäli asiakas olisi kiireinen synkronointihetkellä, eikä hän näin huomaisi uuden jaetun avaimen synkronointia. Tästä syystä pyyntö hylättäisiin väärän jaetun avaimen takia. (5.)

3.8 RADIUS-tilastointi

RADIUS-tilastointi perustuu asiakas-palvelin -malliin. RADIUS-tilastointipalvelin on palvelin asiakkaalle. Tilastointipalvelin voi toimia myös välityspalvelimena välittäen tilastoinnin etäpalvelimelle. Asiakkaan ja palvelimen välinen viestintä on salattua jaetun avaimen avulla, jota ei koskaan lähetetä verkossa. Tilastointiattribuuttien muoto on samankaltainen kuin todennus- ja valtuutusattribuuttien. Useimmat tarjotut palvelut voidaan määrittää käyttäen attribuutti-arvo pareja (Attribute-Value Pairs). (5.)

3.9 Microsoft Network Policy Server

Microsoft Server 2008 sisältää Network Policy and Access Services (NPAS) -roolin. Tähän rooliin sisältyy Network Policy Server (NPS), Health Registration Authority (HRA) sekä Host Credential Authorization Protocol (HCAP). Network Policy Server on Microsoftin toteutus RADIUS-palvelimesta. Se voi toimia RADIUS-palvelimena, RADIUS-välityspalvelimena sekä Network Access Protection (NAP) policy -palvelimena. NPS on yhteensopiva Microsoft Active Directory -tietokantojen kanssa. (6.)

NPAS-rooli asennetaan kuten muutkin palvelinroolit Microsoft Server 2008:ssa. Asennus voidaan suorittaa Server Manager -työkalulla lisäämällä NPAS-rooli palvelimeen. Roolin asentamiseksi valitaan NPS-palvelu roolin palveluiden listalta. (7.)

4 KÄYTÄNNÖN KONFIGUROINTIKÄSKYT

Tietotekniikan koulutusohjelman hallinnoima verkko käyttää pääosin Cisco Systemsin laitteita, jotka käyttävät Ciscon kehittämää Cisco IOS (Internetwork Operating Sys-

tem) -käyttöjärjestelmää. Määrittelyt laitteiden asetuksiin tehdään pääosin komentoriviltä ilman mitään graafista käyttöliittymää. (8.)

Verkon aktiivilaitteisiin voidaan tietyin edellytyksin ottaa etähallintayhteys ns. virtuaalisten pääteyhteyksien kautta käyttäen oletuksen mukaisesti Telnet-protokollaa. Virtuaalilinjat on hyvä määritellä käyttämään Telnetin sijaan SSH-yhteyskäytäntöä, mikä parantaa tietoturvaa merkittävästi. SSH:ta varten on määriteltävä laitteelle nimi komennolla **hostname HOSTNAME**. Laitteella tulee olla domain-nimi, joka määritellään komennolla **ip domain-name Example.com**. Laitteeseen on myös luotava RSA-avainparit viestien salaukseen komennolla **crypto key generate rsa**. SSH kannattaa määritellä käyttämään versiota 2 komennolla **ip ssh version 2**. Jotta saadaan käyttöön SSH:n versio 2, täytyy avainten pituus olla vähintään 1024 bittiä. (9.)

Ongelmatilanteita varten on hyvä luoda myös paikallinen käyttäjä komennolla **username USER secret SECRET**. AAA:n uudempi malli otetaan käyttöön komennolla **aaa new-model**. RADIUS-palvelimille luodaan ryhmä komennolla **aaa group server radius GROUP**. Tähän ryhmään voidaan lisätä yksi tai useampi RADIUS-palvelin komennolla **server-private x.x.x.x key KEY**. Komennossa annettu key on RADIUS:n käyttämä jaettu avain (Shared Secret). Komennossa voidaan myös määritellä muita attribuutteja kuten porttinumerot. Varsinaisesti todennus otetaan käyttöön komennolla **aaa authentication login default group GROUP local**. Näin määriteltynä todennus tapahtuu ensisijaisesti ryhmän sisältämien RADIUS-palvelinten kautta. Mikäli yhteenkään palvelimeen ei saada yhteyttä, todennetaan lopulta paikallisen käyttäjätietokannan kautta. RADIUS vaatii todennuksen rinnalle myös valtuutuksen, joka määritellään komennolla **aaa authorization exec default group GROUP local**. Virtuaalilinjat määritellään käyttämään SSH:ta komennolla **transport input ssh**, sekä todennus otetaan käyttöön komennolla **login authentication default**. (10.)

Mikäli laitteessa on useita IP-osoitteita ja portteja, saatetaan myös vaatia komento **ip radius source-interface INT.** Tämä komento määrittelee mihin porttiin RADIUS-paketit lähetetään, jotta ne osataan lähettää oikealla lähde IP-osoitteella. (10.)

5 TEKNINEN TOTEUTUS

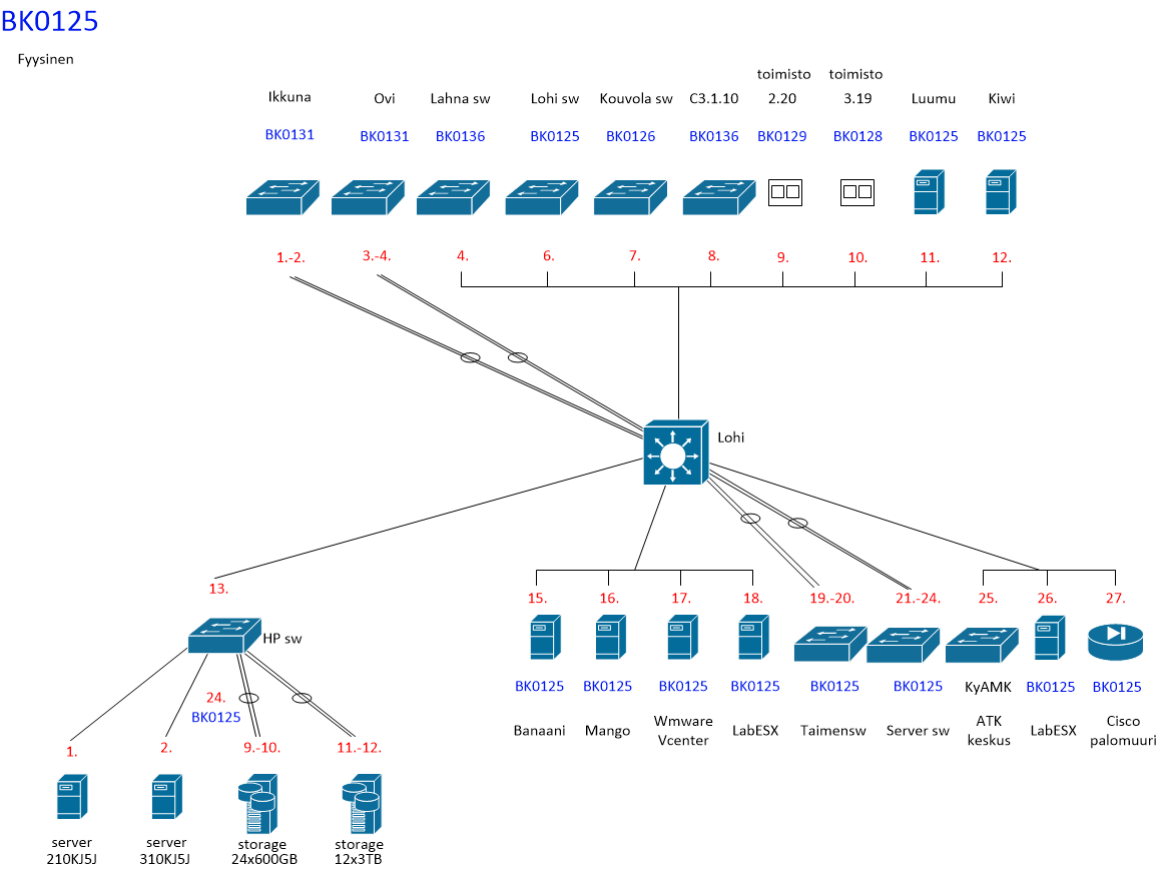
Kymenlaakson ammattikorkeakoulun Tietotekniikan koulutusohjelman osaksi tuleva Kyberturvallisuuslaboratorio lisäsi nykyisen verkon tietoturvatarpeita. Tätä varten

verkon aktiivilaitteiden etähallinnassa päätettiin luopua paikallisista käyttäjätunnuksista ja tunnetuista salasanoista. Tilalle päätettiin ottaa Tietotekniikan koulutusohjelman oma Active Directory -käyttäjätietokanta, jota hyödynnetään käyttäen lisäksi RADIUS-protokollaa.

Active Directory -tietokannan käyttäminen suunnitellusti vaatii Windows Server 2008 R2 -palvelimeen Network Policy Server (NPS) -ominaisuuden asentamisen. Koska verkkoon oli jo aiemmin luotu VPN-yhteyksiä varten RADIUS-palvelin, ei sitä tarvinnut asentaa enää uudelleen. Vanhaan RADIUS-palvelimeen täytyi tehdä uusi politiikka verkkolaitteiden hallintayhteyksille sekä lisätä verkkolaitteet RADIUS-asiakkaiden listaan.

5.1 Tietotekniikan koulutusohjelman verkko

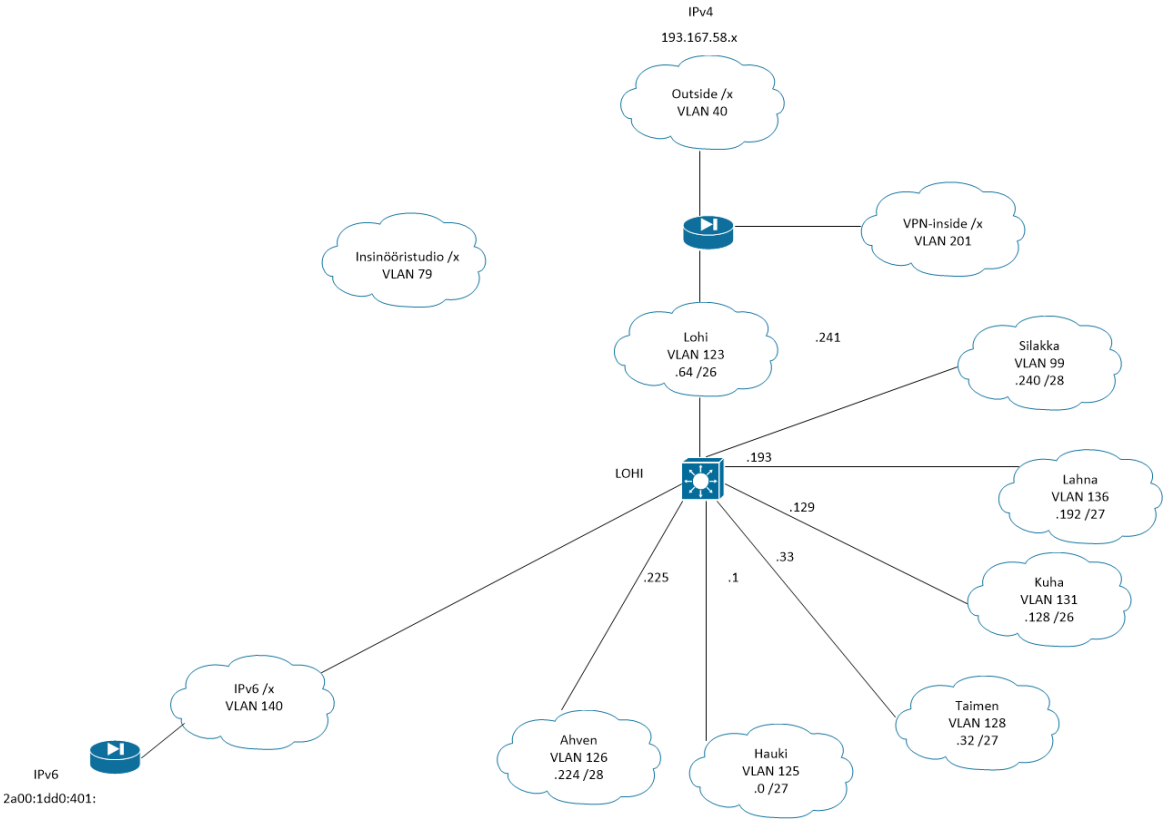
Tietotekniikan koulutusohjelman hallinnoima tietoverkko on kytkinverkko, johon tulee Kyamkin tietohallinnon puolelta IPv4-yhteys sekä SimuNetin puolelta IPv6-yhteys. Tietotekniikan verkossa on käytössä yksi C-luokan kokoinen julkinen IP-osoittealue. Osoitealue on jaettu seitsemään aliverkkoon, jotka muodostavat virtuaalilähiverkkojen (VLAN) osoitteiston. Virtuaalilähiverkot ovat muodostettu käytössä olevien huonetilojen perusteella. Verkkoa kutsutaan kalaverkoksi ja jokaisella virtuaalilähiverkolla on jonkin kalan nimi. Verkon ytimenä on yksi Cisco Systemsin Catalyst 3750 -kytkin, joka toimii yhdyskäytävänä kaikille virtuaalilähiverkoille. Tämä kytkin myös toimii reitittimenä virtuaalilähiverkkojen väliselle liikenteelle. Tästä kytkimestä lähtee linjat muihin verkon kytkimiin sekä osaan palvelimista. Kuva 6 esittää verkon fyysistä topologiaa.



Kuva 6. Tietotekniikan siiven verkon fyysinen topologia (11.)

Ulkoverkkoon eli Internetiin löytyy kaksi eri reittiä. Tärkein yhteyksistä on IPv4-yhteys Kyamkin tietohallinnon kautta Funet-verkkoon, joka on Suomen korkeakoulujen ja tutkimuksen tietoverkko ja palvelee suomalaisia yliopistoja ja ammattikorkeakouluja sekä tutkimuslaitoksia (12). Toinen ulkoinen yhteys toimii IPv6-osoitteilla operaattoriverkkoa simuloivan SimuNet-verkon kautta. SimuNet-verkko rakennettiin Kymenlaakson ammattikorkeakoulun ja KYMP OY:n sekä usean muun yrityksen kanssa yhteistyössä toteutetussa projektissa ja sitä käytetään IPv6-verkkojen tutkimukseen (13). SimuNetissa on käytössä vain IPv6-osoitteet, jotka se saa KYMP OY:ltä.

Sisäverkko on topologialtaan tähti. Siinä on keskuskytkin, johon on yhdistetty useampi kytkin sekä muita laitteita. Liitettyjen kytkinten takaa löytyy palvelimia sekä lukuisia tietokoneita eri luokissa. Tietotekniikan siivessä on myös oma langaton lähiverkko, minkä tukiasemat löytyvät verkosta. Verkon reunoilla on Cisco Systemsin ASA 5510 -palomuurit. Yksi palomuuri on sisäverkon ja tietohallinnon välissä, ja toinen sisäverkon ja SimuNetin välissä. Kuva 7 esittää verkon loogista topologiaa, josta selviää hyvin ulkoverkon yhteydet sekä palomuurien sijainti.



Kuva 7. Tietotekniikan siiven verkon looginen topologia (11.)

5.2 Verkkolaitteiden määrittelyt

Tietotekniikan koulutusohjelman hallinnoiman verkon aktiivilaitteissa oli aiemmin käytössä paikalliset tunnetut salasanat. Yhden laitteen salasanaa kukaan ei tuntenut, joten siihen täytyi suorittaa salasananpalautus toimenpide. Salasananpalautus vaati laitteen uudelleenkäynnistämisen, joten siitä syntyi pieni katkos osaan verkosta. Muuten opinnäytetyön yhteydessä suoritetut toimenpiteet eivät aiheuttaneet häiriöitä verkkoon.

Jotta RADIUS-protokolla toimii, on laitteella oltava vähintään yksi IP-osoite, jolla laitteeseen voidaan muodostaa etähallintayhteys. Laitteessa täytyy olla myös oletusyhdyskäytävä, jotta laitteella on reitti ulospäin. Jokaisessa laitteessa, johon RADIUS-todennus otettiin käyttöön, oli jo ennestään määritelty hallintaosoite sekä oletusyhdyskäytävä niille varatusta virtuaalilähiverkosta.

Koska verkon tietoturvaa haluttiin parantaa, määriteltiin laitteet käyttämään SSH:ta virtuaaliyhteyksiin. Tätä varten täytyi laitteisiin määrittää laitteen nimi, domainin nimi, sekä luoda RSA-avainparit. Laitteissa oli valmiiksi määriteltyinä laitteen sekä do-

mainin nimet. Tietoturvan parantamiseksi otettiin käyttöön SSH:n versio 2, joka parantaa tietoturvaa sekä vaatii pidempiä RSA-avainpareja.

Laitteisiin on aluksi hyvä luoda paikallinen käyttäjä ongelmatilanteita varten. Mikäli laite ei jostain syystä saa yhteyttä RADIUS-pavelimeen, otetaan käyttöön paikallinen käyttäjätietokanta. Paikallista tietokantaa ei kuitenkaan käytetä milloinkaan, jos laite löytää RADIUS-palvelimen. Tämä ei siis luo kovinkaan suurta tietoturva-aukkoa laitteeseen, vaikka paikallisen käyttäjän salasana ei olisi niin hyvin suojattu.

Käyttäjän lisäämisen jälkeen otetaan uusi AAA-malli käyttöön. Tämän jälkeen määritellään RADIUS-palvelimelle palvelinryhmä, sekä lisätään RADIUS-palvelin tähän ryhmään. Palvelin määriteltiin käyttämään uusia porttinumeroita selkeyden vuoksi. Jos porttinumeroita ei erikseen määritellä, laite käyttää automaattisesti vanhoja porttinumeroita. Joissain IOS-versioissa ei ole tukea palvelinryhmille, mutta palvelimet voidaan lisätä myös ilman erillistä ryhmää, jolloin käytetään oletusryhmää. Kun palvelimet on lisätty, otetaan todennus ja valtuutus käyttöön siten, että RADIUS on ensisijainen todennusmenettely ja varalla on paikallisia käyttäjiä. Lisäksi määriteltiin erikseen konsolilinjoille ryhmä, jossa käytetään pelkästään paikallisia käyttäjiä. Lopuksi voidaan määritellä virtuaalilinjat käyttämään oletustodennusta, joka käyttää RADIUS-ta. Konsolilinjalla puolestaan on erikseen määritelty todennus, joka käyttää paikallisia tunnuksia.

Verkon keskuskytkimessä on määriteltynä useita virtuaalilähiverkkoja, joille laite toimii yhdyskäytävänä ja reitittimenä. Tätä varten laitteessa on oltava IP-osoitte jokaisessa virtuaalilähiverkossa. Tästä syystä laitteeseen täytyy määritellä lisäkomento, joka kertoo laitteelle oikean liitäntäportin. Muuten laite saattaa käyttää väärää IP-osoitetta palvelimelle lähettämissään RADIUS-paketeissa.

Opinnäytetyön myötä laitteisiin tehdyt määrittelyt olivat melko lyhyet. Parissa laitteessa olleet IOS-versiot eivät tukeneet RADIUS-palvelinryhmien luontia, joten niissä käytettiin oletusryhmää. Keskuskytkimeen määriteltiin seuraavat komennot:

```
lohi(config)#username admin secret SECRET1
lohi(config)#enable secret SECRET2
lohi(config)#crypto key generate rsa
lohi(config)#ip ssh version 2
```

```
lohi(config)#aaa new-model
lohi(config)# radius-server host 193.167.58.25 auth-port 1812 acct-port 1813 key
SHAREDSECRET
lohi(config)#ip radius source-interface Vlan99
lohi(config)#aaa authentication login default group radius local
lohi(config)#aaa authentication login CONSOLE local
lohi(config)#aaa authorization exec default group radius local
lohi(config)#line con 0
lohi(config-line)#login authentication CONSOLE
lohi(config)#line vty 0 15
lohi(config-line)#transport input ssh
lohi(config-line)#login authentication default
```

Keskuskytkimessä ja yhdessä toisessa kytkimessä olleet IOS-versiot eivät tukeneet erillisiä RADIUS-palvelinryhmiä, joten niihin määriteltiin suoraan RADIUS-palvelin ilman erillistä ryhmää. Muissa laitteissa löytyi tuki palvelinryhmille ja niitä myös käytettiin hyväksi. Keskuskytkimen lisäksi verkossa oli viisi muuta kytkintä, joihin määriteltiin pääosin samanlaiset konfiguraatiot. Näihin viiteen kytkimeen ei tarvinnut määrittää komentoa **ip radius source-interface**, koska laitteissa oli vain yksi IP-osoite hallintatarkoituksessa. Keskuskytkimen ja yhden työryhmäkytkimen tarkemmat osakonfiguraatiot löytyvät liitteinä, joista selviää laitteisiin tehdyt muutokset.

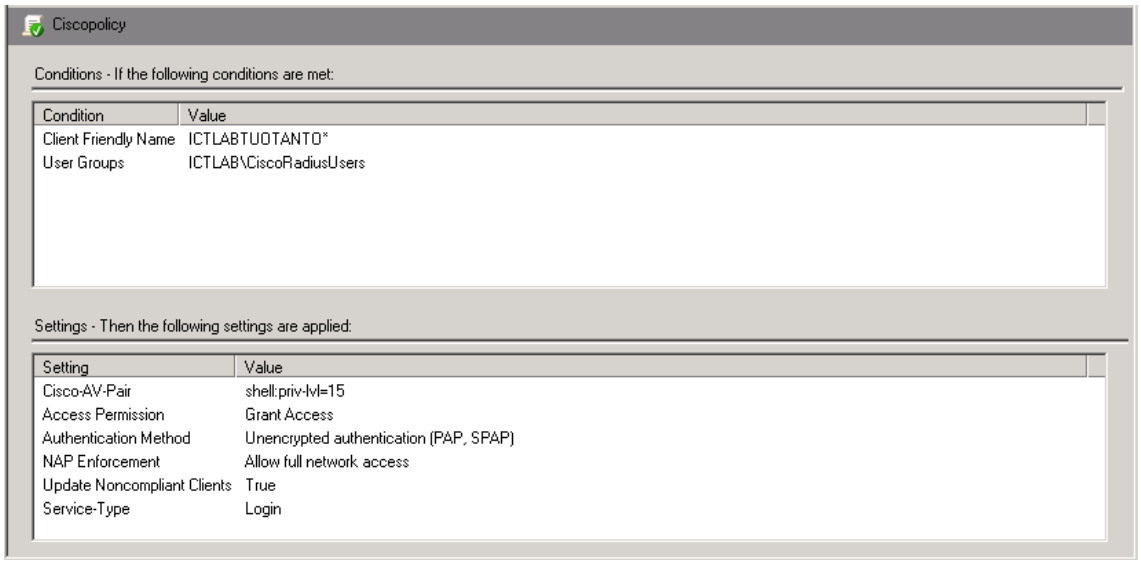
5.3 Palvelimen määrittelyt

RADIUS-palvelimena toimii verkon Active Directory -palvelin. Palvelimen käyttöjärjestelmänä on Windows Server 2008 R2. Tähän palvelimeen oli aiemmin asennettu VPN-yhteyksiä varten Network Policy Server, joten sitä ei tarvinnut asentaa uudelleen.

Active Directoryn käyttäjätietokantaan luotiin uusi käyttäjäryhmä, joille sallitaan etäyhteyden muodostaminen verkon aktiivilaitteisiin. Tähän ryhmään lisättiin olemassa ollut Henkilökunta-ryhmä sekä testitarkoituksessa opinnäytetyön tekijä. Ryhmään on myöhemmin helppo lisätä tai poistaa käyttäjiä tarpeen mukaan esimerkiksi jotain projektia varten.

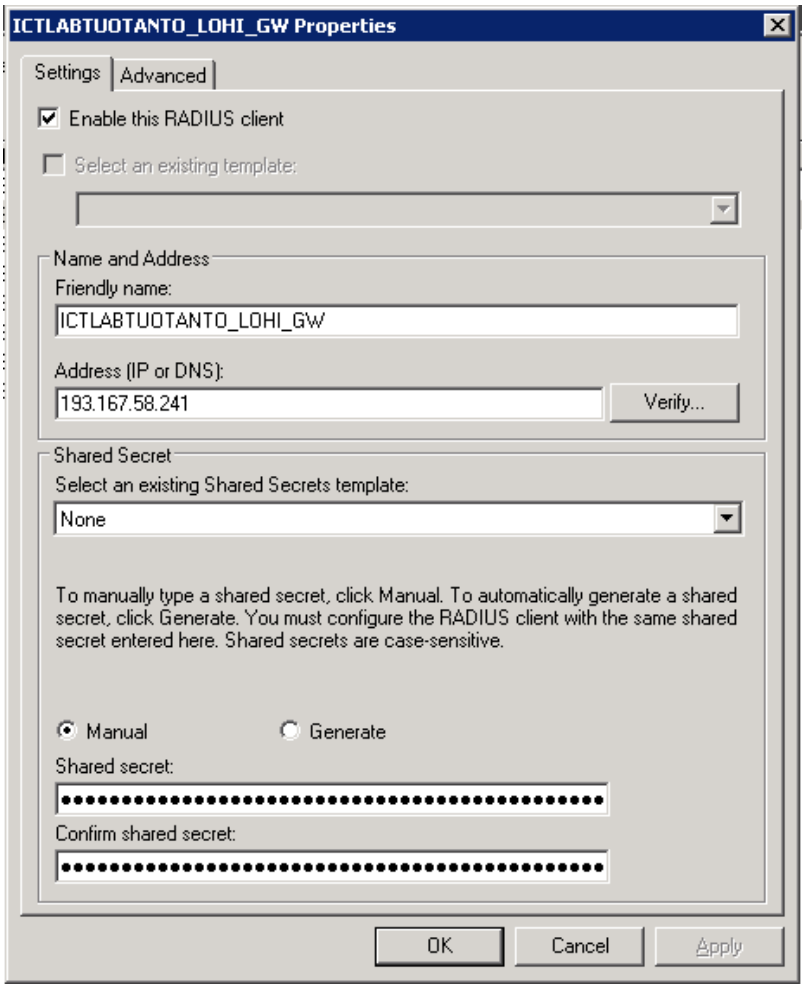
Palvelimen Connection Request Policies -osasta täytyy poistaa PPP sekä Framed asetukset vakiona olevasta politiikasta, jotta ne eivät ohita muita määrittelyjä.

Cisco Systemsin laitteita varten täytyy luoda uusi Network Policy -politiikka. Tällä politiikalla määritetään mitkä laitteet käyttävät politiikkaa ja käyttäjät, joiden sallitaan politiikan ottaa hallintayhteys laitteeseen, sekä paljon ehtoja ja asetuksia joita yhteydelle asetetaan. Koska Ciscon IOS käyttää todentamiseen PAP:ia, tulee vähintään se valita käytetyistä todennusmenetelmistä. Laitteiksi määriteltiin kaikki verkon laitteet nimen perusteella ja käyttäjiksi määriteltiin aiemmin luotu käyttäjäryhmä. Politiikkaan on myös mahdollista lisätä ehtoja päivämäärästä, kellon ajasta, yhteyttä muodostavasta laitteesta sekä portin tyypistä. Lopuksi määritellään sallitulle yhteydelle asetukset. Myös näistä asetuksista poistetaan PPP sekä Framed. Tilalle lisätään normaaliasetuksista **Service-Type:Login**. Lisäksi määritellään valmistajakohtaisista asetuksista Ciscon attribuutti-arvo pari, jolle annettiin arvo **shell:priv-lvl=15**. Kuva 8 näyttää yhteenvedon määritetystä politiikasta.



Kuva 8. Luodun Network Policyn määrittelyt

Jokainen RADIUS-todennusta käyttävä laite täytyy lisätä RADIUS-asiakkaiden listaan. Asiakkaille annetaan nimi, osoite sekä jaettu salaisuus. Lisäksi voidaan määritellä joitain valmistajakohtaisia asetuksia. Nimeksi annettiin alkuosaltaan sama nimi, jotta siihen on helppo viitata käytetyssä Network Policyssä. Osoitteeksi annettiin hallinta VLANista laitteelle jo aiemmin määritelty IPv4-osoite. Jaettu avain generoitiin jokaiselle laitteelle generaattorilla. Kuva 9 esittää asiakkaan määrittelyjä.



Kuva 9. Asiakaslaitteen määrittelyt

6 YHTEENVETO

Tämän opinnäytetyön tärkeimpänä tavoitteena oli tutustua RADIUS-protokollaan ja toteuttaa valmiiseen Microsoft Active Directory -tietokantaan perustuva todennus, jolla valvotaan verkon aktiivilaitteiden etähallintayhteyksien käyttäytymistä. Työn alkuvaiheessa RADIUS-protokollan ja Active Directoryn yhteistyöhön tutustuttiin rakentamalla testiympäristö ICT-laboratorion laitteilla. Harjoitteluvaiheen jälkeen ryhdyttiin rakentamaan vastaavaa järjestelmään tuotantoverkon puolelle. Täysin toivottuun

lopputulokseen ei päästy, koska IPv6 osoitteita käyttäviin SimuNetin laitteisiin ei saatu toteutettua RADIUS-todennusta. Tämä johtui erittäin vähäisestä saatavilla olevasta tiedosta RADIUS-todennuksen käyttämisesti IPv6-verkoissa, sekä laitteiden puutteellisesta tuesta IPv6-protokollalle.

Opinnäytetyö perehdytti RADIUS-protokollaan ja opetti ymmärtämään sen toimintaa. Vaikka RADIUS on vanha protokolla, se on edelleen käyttökelpoinen monissa toteutuksissa. Kun RADIUS-protokollaan yhdistetään Active Directory -tietokanta, saadaan erittäin järkevästi toimiva todennus verkkolaitteille. Jos käytetyissä Cisco Systemsin verkkolaitteissa olisi PAP:n tilalla jokin tuoreempi todennusmenetelmä, saataisiin laitteille vielä paljon tietoturvallisempi etähallinta.

Todennuksen toteutus sujui teorian opiskelun avulla hyvin. Pieni ongelma esiintyi kuitenkin verkossa käytetyssä keskuskytkimessä, jossa oli useita IP-osoitteita. Ongelmaa tutkiessa huomattiin, että paketit lähtivät palvelimelle väärällä lähdeosoitteella. Tämä ongelma ratkesi lisäämällä komento, jolla määritellään minkä portin osoitetta käytetään lähetettävien pakettien lähdeosoitteena. Toinen todella suuri haaste oli toteuttaa vastaava todennus SimuNettiin. Koska SimuNet on täysin IPv6-osoitteita käyttävä verkko, olisi myös RADIUS täytynyt toteuttaa IPv6-osoitteilla. Tämän toteuttamiseen ei kuitenkaan löytynyt juuri mitään tietoa käytettyjen verkkolaiteiden osalta. On myös hyvin mahdollista, että käytetyt laitteet eivät tukeneet RADIUS-todennusta IPv6-verkossa.

Jatkokehityksenä RADIUS:n toimintaan IPv6-verkoissa tulisi perehtyä. Tietoa alkaa varmasti löytyä enemmän, kunhan IPv6 otetaan vielä enemmin käyttöön. Uskon, että IPv6-verkon toteutus esimerkiksi SimuNettiin tarjoaa ainakin uuden projektin.

LÄHTEET

1. Convery, S. 2007. Network Authentication, Authorization, and Accounting: Part One. Saatavissa: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-1/101_aaa-part1.html [viitattu 12.2.2014]

2. Juniper. 2008. RADIUS Overview. Saatavissa: http://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/Concepts2.html [viitattu 12.2.2014]

3. Cisco. 2006. How Does RADIUS Work? Saatavissa: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html [viitattu 12.2.2014]

4. The Internet Society. 2000. RFC2865. Saatavissa: http://tools.ietf.org/search/rfc2865 [viitattu 12.2.2014]

5. Hassell, J. 2002. RADIUS. Sebastopol: O'Reilly Media.

6. Microsoft. 2012. Network Policy and Access Services. Saatavissa: http://technet.microsoft.com/en-us/network/bb545879.aspx [viitattu 6.3.2014]

7. Microsoft. 2012. Install Network Policy Server (NPS). Saatavissa: http://technet.microsoft.com/en-us/library/cc725658%28v=ws.10%29.aspx [viitattu 6.3.2014]

8. Cisco. 2014. Cisco IOS Technologies. Saatavissa: http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-technologies/index.html [viitattu 11.4.2014]

9. Arthur. 2012. How to: Setup SSH terminal access on Cisco IOS. Saatavissa: http://blog.arwin.me/os/cisco/how-to-setup-ssh-terminal-access-on-cisco-ios/ [viitattu 6.3.2014]

10. Arthur. 2012. How to: Setup Cisco IOS to authenticate via Active Directory. Saatavissa: http://blog.arwin.me/os/cisco/how-to-setup-cisco-ios-to-authenticate-via-active-directory/ [viitattu 6.3.2014]

11. Tuntematon. 2013. Kymenlaakson ammattikorkeakoulun Tietotekniikan siiven dokumenttikuvia. Saatavissa: Kymenlaakson Ammattikorkeakoulun ICT-Laboratorion sisäverkko.

12. CSC - Tieteen tietotekniikan keskus. 2014. Funet yhdistää tutkimusyhteisön. Saatavissa: http://www.csc.fi/hallinto/funet/esittely [viitattu 11.4.2014]

13. Kettunen, M. 2014. SimuNet-hanke. Saatavissa: http://www.ictlab.kyamk.fi/index.php/simunet-hanke [viitattu 6.3.2014]

LOHI-GW -LAITTEEN OSAKONFIGURAATIO

```
Current configuration : 10588 bytes
!
hostname lohi
!
username admin secret 5
!
aaa new-model
!
aaa authentication login default group radius local
aaa authentication login CONSOLE local
aaa authorization exec default group radius local
!
ip domain-name ictlab.kyamk.fi
!
ip ssh version 2
!
ip radius source-interface Vlan99
!
radius-server host 193.167.58.25 auth-port 1645 acct-port 1646 key
!
line con 0
 logging synchronous
 login authentication CONSOLE
line vty 0 4
 logging synchronous
 transport input ssh
line vty 5 15
 logging synchronous
 transport input ssh
!
end
```

IKKUNA-SW -LAITTEEN OSAKONFIGURAATIO

```
Current configuration : 6114 bytes
!
hostname Ikkuna
!
username admin secret 5
!
aaa new-model
!
aaa group server radius ADAUTH
 server-private 193.167.58.25 auth-port 1812 acct-port 1813 key
!
aaa authentication login default group ADAUTH local
aaa authentication login CONSOLE local
aaa authorization exec default group ADAUTH local
!
ip domain-name ictlab.kyamk.fi
!
ip ssh version 2
!
line con 0
 logging synchronous
 login authentication CONSOLE
line vty 0 4
 logging synchronous
 transport input ssh
line vty 5 15
 logging synchronous
 transport input ssh
!
end
```